Footprinting

Cybersecurity

2025-2026

Linde Nouwen

KdG

University of Applied Sciences and Arts

~Reconnaissance

- Information discovery on the client/organization
- 2 types:
  - Active: direct interaction with target
  - Passive: only user-like interaction with target

Active Footprinting

- Ping sweeps
- Network mapping
- Social engineering
- Host discovery
- Port scanning

Passive Footprinting

- Ads/ job openings -> technology
- Who-IS (domain/contact info)
- Surfing to their website like a normal user
- Social networks
- Robots.txt

Passive footprinting

Google Dorks

- https://en.wikipedia.org/wiki/Google_hacking
- https://jarnobaselier.nl/google-dorks
- https://sansorg.egnyte.com/dl/f4TCYNMgN6
- https://www.exploit-db.com/google-hacking-database

Google Dorks: operators

+ (plus symbol): is used to include words that because they are very common are not included on Google searchresults.

- ❖ For example, say that you want to look for company The X, given that the article "the" is very common, it is usually excluded from the search. If we want this word to be included, then we write our search text like this: Company +The X

- (minus symbol): is used to exclude a term from results that otherwise could include it.

- ❖ For example, if we are looking for banking institutions, we could write: banks - furniture

"" (double quotes): if we need to find a text literally, we framed it in double quotes.

- ❖ Example: "Company X"

~ (tilde): placing this prefix to a word will include synonyms thereof.

- ❖ For example, search by ~company X willalso include results for organization X

OR: This allows you to include results that meet one or both criteria.

- ❖ For example, "Company X General Manager" OR "Company X Systems Manager"

site: allow to limit searches to a particular Internet site. Example: General Manager site:companyX.com

link: list of pages that contain links to the url.

- ❖ For example, searching for link:companyX.com gets pages that contain links to company X website.

filetype: or **ext:** allows you to search by file types.

- ❖ Example: Payment roles + ext:pdf site:empresax.com

allintext: get pages that contain the search words within the text or body thereof.

- ❖ Example: allintext: Company X

inurl: shows results that contain the search words in the web address (URL).

- ❖ Example: inurl: Company X

NS lookup

- DNS-tool
- DNS = Domain name to IP
- Useful options
  - "server" points to specific DNS-server
  - "set" allows to query DNS for specific types (MX,NS,…)
  - "ls" to check domain-addresses
  - Alternative: dnsrecon (Linux) or dnsdumpster (web)

WHOIS

- Domain ownership
  - Domain name
  - Registrant
    - Name
    - Email address
    - Physical address
    - Contact phone number
    - Term
    - Sometimes even payment information
- Database to retrieve information: http://whois.arin.net

Varia

- See what technology, plugins,… have been used to build the website
  - Browser extensions: Builtwith and Wappalyzer
  - Linux command tool: whatweb
- Copy the entire website: hTTrack
- Subdomain enumeration with Sublist3r (not using subbrute)
- Checking if there is a waf: wafw00f
- A lot of website recon: Netcraft (but paid features)
- Email harvesting with theHarvester

Active footprinting

DNS records

- A - Resolves a hostname to an IPv4 address
- AAAA - Resolves a hostname to an IPv6 address
- NS - Reference to the domain’s nameserver
- MX - Resolves a domain to a mail server
- CNAME - Used for domain aliases
- TXT - Text record
- HINFO - Host information
- SOA - Domain authority
- SRV - Service records
- PTR - Resolves an IP address to a hostname

DNS interrogation

- The process of enumerating DNS records for a specific domain
- Use dnsenum command in Linux
- Alternative: *fierce*

Nmap

- A powerful network scanning tool used for security auditing
- Helps discover hosts and services on a computer network
- Widely used by penetration testers and network administrators
- Open-source and available on multiple platforms

Nmap: host discovery

- -sn option sends various packets to discover hosts (run with sudo)
- For Windows, you often need the –Pn option (windows systems block ping probes by default
- -v option for a more verbose output
- Possibility to put output in a file:
  - -oN puts the output in a file like it is shown on the screen
  - -oX delivers an XML format (for importing into other tools, like Metasploit)

Nmap: port scanning

- Without any options, nmap scans the 1000 most commonly used ports
- -p- option: entire port range
- -p[start]-[finish]: specific port range
- -p[ports in comma-separated list]: specific ports
- -F: 100 most commonly used ports
- -sU: UDP port scan